

# POLYNOMIAL ARITHMETIC DEVICE, DEVICE FOR CALCULATING ORDER OF ELLIPTIC CURVE, DEVICE FOR GENERATING ELLIPTIC CURVE, AND CRYPTOGRAPHIC SYSTEM FOR ELLIPTIC CURVE

**Publication number:** JP2000321979 (A)

**Publication date:** 2000-11-24

**Inventor(s):** FUDA YUICHI

**Applicant(s):** MATSUSHITA ELECTRIC IND CO LTD

**Classification:**

- international: **G09C1/00; G06F7/72; G09C1/00; G06F7/60;** (IPC1-7): G09C1/00; G06F7/72

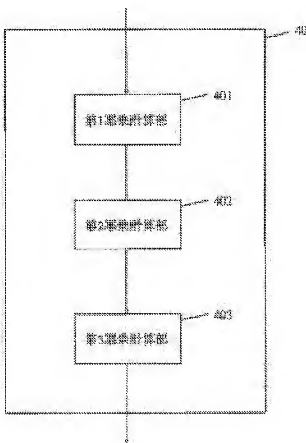
- European:

**Application number:** JP19990133814 19990514

**Priority number(s):** JP19990133814 19990514

## Abstract of JP 2000321979 (A)

**PROBLEM TO BE SOLVED:** To permit high velocity and safe cryptography method and signature method by providing a polynomial arithmetic device with first the second power calculation means and allowing the second power calculation means to use the result outputted from the first power calculation device. **SOLUTION:** In this polynomial arithmetic device, a first power calculation part 401 calculates and outputs  $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$  in one variable polynomial residue ring  $R=GF(q)[X]/r(X)$  with  $GF(q)$  ( $q=p^n$ , where  $p$  is prime number, and  $p^n$  means  $n$ th power of  $p$ ) as a finite body,  $X$  as a variable, and a solution as a previously given  $r(X)$  (degree  $d$ ) being a coefficient  $GF(q)$ . A second power calculation part 402 outputs  $X^q$  by inputting  $X$  belonging to  $R$  and  $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$  of the first power calculation part 401. A third power calculation part 403 calculates  $f(X)^{7((q-1)/2)}$  by inputting  $X$  belonging to  $R$  and  $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$  of the first power calculation part 401.



Data supplied from the **esp@cenet** database — Worldwide

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-321979

(P2000-321979A)

(43) 公開日 平成12年11月24日 (2000. 11. 24)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	キーワード <sup>*</sup> (参考)
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 Z 5 J 1 0 4
G 0 6 F 7/72		G 0 6 F 7/72	6 5 0 A 9 A 0 0 1

審査請求 未請求 請求項の数 8 O L (全 9 頁)

(21) 出願番号 特願平11-133814

(22) 出願日 平成11年5月14日 (1999. 5. 14)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 布田 裕一

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100097445

弁理士 岩橋 文雄 (外2名)

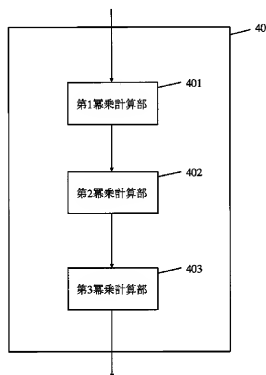
Fターム(参考) 5J104 AA22 AA25 JA25 JA29 NA16  
NA189A001 B802 E803 FF01 GG01 GG11  
GG22 KK12 LL02 LL03

(54) 【発明の名称】 多項式演算装置、楕円曲線点数計算装置、楕円曲線生成装置及び楕円曲線暗号システム

(57) 【要約】

【課題】 本発明は、高速な多項式演算装置を提供し、それにより高速に安全な楕円曲線を生成することのできる楕円曲線生成装置を提供する。

【解決手段】 有限体GF(q) ( $q=p^n$ , p:素数) 上の多項式  $r(X)$  を法とする 1変数多項式剰余環  $R=GF(q)[X]/(r(X))$  において、Rに属する多項式X、 $f(X)$  を入力とし、Rに属する多項式  $X^q$ 、 $f(X)^{((q-1)/2)}$  を出力する多項式演算装置であって、前記多項式Xに対して、 $X^p$ 、 $X^{(2p)}$ 、 $X^{(3p)}$ 、...、 $X^{((d-1)p)}$  を計算する第1乗算部と、 $f(X)^{((q-1)/2)}$  を計算する第2乗算部を備え、前記第2乗算計算手段は、前記第1乗算計算手段から出力される結果を用いる。



## 【特許請求の範囲】

【請求項1】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上の予め与えられた多項式r(x) (次数d)を法とする1変数多項式剰余環 $R=GF(q)[X]/(r(X))$ において、Rに属する多項式X、f(X)を入力とし、Rに属する多項式 $X^q$ 、 $f(X)^{((q-1)/2)}$ を出力する多項式演算装置であって、

前記多項式Xに対して、 $X^p$ 、 $X^{(2p)}$ 、 $X^{(3p)}$ 、…、 $X^{(p-1)p}$

$$f(X)^{((p^2-1)/2)} = (f(X)^{((p-1)/2)})^p \times f(X)^{((p-1)/2)}$$

$$f(X)^{((p^3-1)/2)} = (f(X)^{((p^2-1)/2)})^p \times f(X)^{((p-1)/2)}$$

…

$$f(X)^{((p^n-1)/2)} = (f(X)^{((p^{n-1}-1)/2)})^p \times f(X)^{((p-1)/2)}$$

により計算することを特徴とする請求項1記載の多項式演算装置。

【請求項3】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上の楕円曲線を入力とし、前記楕円曲線の位数を出力する楕円曲線位数計算装置であって、予め与えられた初期値を設定する初期値設定部と、位数の情報を求める楕円曲線位数情報計算部と、前記楕円曲線位数情報計算部の終了判定を行う計算終了判定部と、前記楕円曲線位数情報計算部から出力される情報を用いて楕円曲線の位数を決定する楕円曲線位数決定部とを備え、前記楕円曲線位数情報計算部は、請求項1に記載の多項式演算装置を有することを特徴とする楕円曲線位数計算装置。

【請求項4】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上の楕円曲線を入力とし、前記楕円曲線の位数を出力する楕円曲線位数計算装置であって、予め与えられた初期値を設定する初期値設定部と、位数の情報を求める楕円曲線位数情報計算部と、前記楕円曲線位数情報計算部の終了判定を行う計算終了判定部と、前記楕円曲線位数情報計算部から出力される情報を用いて楕円曲線の位数を決定する楕円曲線位数決定部とを備え、前記楕円曲線位数情報計算部は、請求項2に記載の多項式演算装置を有することを特徴とする楕円曲線位数計算装置。

【請求項5】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を出力する楕円曲線生成装置であって、予め与えられた楕円曲線設定値に基づいて楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部とを備え、

前記楕円曲線位数計算部は、請求項3に記載の楕円曲線位数計算装置を有することを特徴とする楕円曲線生成装置。

【請求項6】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を出力する楕円曲線生成装置であって、予め与

((d-1)p)を計算する第1乗計算手段と、 $f(X)^{((q-1)/2)}$ を計算する第2乗計算手段とを備え、

前記第2乗計算手段は、前記第1乗計算手段から出力される結果を用いることを特徴とする多項式演算装置(ただし、 $p^n \nmid 3p$ のn乗を示す)。

【請求項2】 前記第2乗計算手段は、 $f(X)^{((p-1)/2)}$ を計算する中間計算を行って、前記第1乗計算手段から出力される結果を用いて、

えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部とを備え、

前記楕円曲線位数計算部は、請求項4に記載の楕円曲線位数計算装置を有することを特徴とする楕円曲線生成装置。

【請求項7】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を用いる楕円曲線暗号システムであって、予め与えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部とを備え、

前記楕円曲線位数計算部は、請求項3に記載の楕円曲線位数計算装置を有する楕円曲線生成装置により生成されることを特徴とする楕円曲線暗号システム。

【請求項8】 予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を用いる楕円曲線暗号システムであって、予め与えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部とを備え、

前記楕円曲線位数計算部は、請求項4に記載の楕円曲線位数計算装置を有する楕円曲線生成装置により生成されることを特徴とする楕円曲線暗号システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は情報セキュリティ技術としての暗号技術及び、誤り訂正技術に関するものであり、特に、楕円曲線を用いて実現する暗号及びデジタル署名技術及び、楕円曲線を用いて実現する誤り訂正技術に関するものである。

【0002】

【従来の技術】秘密通信方式とは、特定の通信相手以外に通信内容を漏らすことなく通信を行なう方式である。またデジタル署名方式とは、通信相手に通信内容の正当性を示したり、本人であることを証明する通信方式である。この署名方式には公開鍵暗号とよばれる暗号方式を用いる。公開鍵暗号は通信相手が多数の時、通信相手ごとに異なる暗号鍵を容易に管理するための方式であり、多数の通信相手と通信を行なうのに不可欠な基盤技術である。簡単に説明すると、これは暗号化鍵と復号化鍵が異なり、復号化鍵は秘密にするが、暗号化鍵を公開する方式である。この公開鍵暗号の安全性の根拠に用いられるものに離散対数問題がある。離散対数問題には代表的に、有限体上定義されるもの及び楕円曲線上定義されるものがある。これはNeal Koblitz, "A Course in Number theory and Cryptography", Springer-Verlag, 1987に詳しく述べられている。楕円曲線上の離散対数問題を以下に述べる。

【0003】(楕円曲線上の離散対数問題)  $E(\mathbb{GF}(q))$  を有限体  $\mathbb{GF}(q)$  ( $q=p^n$ ) 上定義された楕円曲線  $E$  とし、 $E$  の位数が大きな素数で割れる元  $G$  をベースポイントとする。このとき、 $E$  の与えられた元  $V$  に対して、

$Y=xG$  となる整数  $x$  が存在するならば  $x$  を求めよ。

【0004】楕円曲線の離散対数問題には様々な解読法が提案されており、それらに対して安全な楕円曲線を構成する必要がある。現存するすべての解読法に対して安全な楕円曲線は有限体  $\mathbb{GF}(q)$  上の楕円曲線の場合、位数が  $q-1, q, q+1$  でないこと及び位数が大きい素因数をもつことである。このとき、解読に必要な計算時間は位数の最大素因数に関する指数時間である(情報処理学会監修、岡本龍明、太田和夫共編、"暗号・ゼロ知識証明、数論", 共立出版, 1995, 155ページ~156ページ参照)。したがって、位数が素数である楕円曲線を用いると暗号の安全性が最大になる。楕円曲線の安全性は、その楕円曲線の位数を調べるにより確認できる。

【0005】楕円曲線の従来の構成法として、

- (1) CM法を用いる構成法
  - (2) 位数計算アルゴリズムを用いる構成法
- がある。(1)は楕円曲線の構成が簡単であるが、ランダムに楕円曲線を構成できない。これはA. Miyaji, "On Ordinary Elliptic Curve Cryptosystems", ASIACRYPT '91, Springer-Verlag, 1991, 460ページ~469ページ(訳)。 (2)はランダムに楕円曲線を構成できるが、構成時間が長い。

【0006】(従来例1) 図4は従来例1の位数計算アルゴリズムを用いる楕円曲線生成装置を示すブロック図である。(N. Koblitz, "Elliptic Curve Implementation of Zero-Knowledge Blobs", J. Cryptology, vol. 4, No. 3, 1991, 207ページ~213ページ参照)。従来例1の楕円曲線生成装置は、乱数生成部101と、楕円曲線設定部102と、楕円曲

線位数計算部103からなる。以下、従来例1の動作を説明する。

step1: 乱数生成部101

乱数を発生する。

step2: 楕円曲線設定部102

step1により生成した乱数に対して、楕円曲線を設定する。

step3: 楕円曲線位数計算部103

step2の楕円曲線の位数を計算する。

step4: 楕円曲線条件判定部104

step2の楕円曲線を与えられた条件で判定する。与えられた条件を満たすときのみ、楕円曲線のパラメータを出力する。満たさないとき、step1に戻る。

【0007】上記で述べたように位数計算アルゴリズムを用いる構成法は計算時間が長い。上記従来例1で最も計算時間を要する箇所がstep3の楕円曲線位数計算部である。楕円曲線の位数を計算するアルゴリズムの一つに Schoof のアルゴリズムがある。このアルゴリズムは多項式時間で構成されるが、実用的な計算時間ではない。Schoof のアルゴリズムはElkies, Atkinによって、SEA アルゴリズムとして改良されている。

【0008】(従来例2) 図5は従来例2のSEA アルゴリズムによる楕円曲線位数計算装置の構成を示すブロック図で、R. Lercier, F. Morain, "Counting the number of points on elliptic curves over finite fields: strategies performances", EUROCRYPT '95, Springer-Verlag, 1995, 79ページ~94ページにあるものである。従来例2の楕円曲線位数計算装置は、初期値設定部201と、楕円曲線位数情報計算部202と、計算終了判定部203と、楕円曲線位数決定部204からなる。以下、従来例2の動作を説明する。

【0009】 $p$  を素数、 $q=p^n$  とし、 $\mathbb{GF}(q)$  上の楕円曲線  $E$  の方程式を  $y^2=x^3+ax+b$  とする。ここで、 $x/a$  は  $x/a$  乗を示す。求める位数を  $m$  とし、 $t$  を  $m=q+1-t$  を満たすものとする。 $f(x)=x^3+ax+b$  とする。

step1: 初期値設定部201

$l:=2$  とする。

step2: 楕円曲線位数情報計算部202

$t \bmod l$  を求める。その際、Modular多項式  $\Phi_l(T)$  の一変数  $T$  の多項式環  $\mathbb{GF}(q)[T]$  における因数分解の一次因子の数に対応して以下のように求める。 Modular多項式は、R. Schoof, "Counting points on elliptic curve over finite fields", Journal de Theorie des Nombres de Bordeaux 7, 1995, 219ページ~254ページに詳しく述べられている。

【0010】step2-1. 一次因子の数が2のとき  $t \bmod l$  を求める。さらに、Isogeny cycle 法により、 $t \bmod l^n$  ( $n=2, 3, \dots$ ) を求める。Isogeny cycle 法は、J. M. Couveignes, F. Morain, "Schoof's algorithm and isogeny cycles", ANTS-1, Lecture Notes in Computer Science

ce 877, Springer-Verlag, 1994, 43ページ～58ページに詳しく述べられている。

【0011】step2-2. 一次因子の数が1または141のとき  $t \bmod 1$  を求める。さらに、Isogeny cycle 法により、 $t \bmod 1^n (n=2, 3, \dots)$  を求める。このとき、Isogeny cycle 法を適用可能であるか判定する。

【0012】step2-3. 一次因子の数が0のとき  $t \bmod 1$  の取り得る値を集合  $\{0, 1, \dots, l-1\}$  から絞り込む。

step3: 計算終了判定部203

$11^n(n1) \times 12^n(n2) \times \dots \times 1k^n(nk) < 4 \times q^{(1/2)}$  であるとき  $(11, 12, \dots, 1k)$  は素数であり、 $1k=1$ 、 $1=(1)$  の次の素数)として、step2に戻る。それ以外は次のstep4へ進む。

step4: 楕円曲線位数決定部204

match&sortアルゴリズムにより、位数を確定し、出力する。match&sortアルゴリズムは、R. Lercier, "Algorithmique des courbes elliptiques dans les corps finis", These, Ecole Polytechnique-LIX, 1997 に詳しく述べられている。

【0013】step3の判定はstep2で小さい素数1kに対して、 $t \bmod 1k^n (nk)$  まで求めていると仮定している。step2-1, step2-2では  $t \bmod 1^n (n=1, 2, 3, \dots)$  を求めるがこれはフロベニウス写像と呼ばれる写像の固有値を計算することによってできる。具体的には楕円曲線E上の1等分点  $(X, Y)$  を用いて、以下の式を求める。

【0014】 $(X^q, Y^q) = k(X, Y)$

ここで、 $k(X, Y)$  は点  $(X, Y)$  の楕円曲線上のk倍点であり、 $Y^2 - f(X) = X^3 + aX + b$  である。上式の計算は  $X$  を変数とし、 $GF(q)$  係数である多項式をある多項式法とする  $X$  に関する1変数多項式剰余環上の楕円曲線演算によって行う。上式のkを求めるため、上式左辺の  $X^q$  と  $Y^q = Y \times Y^{(q-1)}$  を求める必要がある。このため、 $X^q$  と  $Y^{(q-1)} = f(X)^{((q-1)/2)}$  の計算を行う。これらの計算に最も時間を必要とする。  $X^q$  以下のアルゴリズムを用いて求められることが知られている。

【0015】(従来例3) 図6は従来例3の多項式演算装置の構成を示すブロック図である。従来例3の多項式演算装置は、第1乗算部301と、第2乗算部302からなる。以下、従来例3の動作を説明する。

【0016】法となる多項式を  $r(X)$ 、その次数を  $d$  とする。

step1: 第1乗算部301

$X^p$ 、 $X^{(2p)}$ 、 $X^{(3p)}$ 、 $\dots$ 、 $X^{((d-1)p)} \bmod r(X)$  を求める。

step2: 第2乗算部302

$X^{(p^2)}$ 、 $X^{(p^3)}$ 、 $\dots$ 、 $X^{(p^n)}$  を求める。

【0017】step2では、 $GF(q)$  係数である多項式  $g(X)$  に対して、

$(g(X))^p = g(X^p)$

となることを利用している (D.E. Knuth 著, 中川圭介訳, "準数値演算/算術演算", KNUIT 第4分冊, サイエンス社, 26ページ～267ページ参照)。この性質より、 $g(X)$  の  $X, X^2, \dots, X^{(d-1)}$  を第1乗算部で求めた  $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$  に置き換えることで、 $(g(X))^p$  が得られる。

【0018】このように、 $X^q$  を求めるアルゴリズムは存在するが、 $Y^{(q-1)}$  を求める有効なアルゴリズムが発表されていないため、単に従来の乗算を用いた計算を行う。しかし、乗算は計算量が大きいため、SEA アルゴリズムの計算量が大きくなるという問題がある。

【0019】

【発明が解決しようとする課題】楕円曲線暗号システムにおいて、安全な楕円曲線パラメータを生成することは重要である。そのために、楕円曲線生成装置を用いる。

【0020】位数計算アルゴリズムを用いる楕円曲線の生成装置では、位数計算部の実行時間が長い。位数計算アルゴリズムの従来技術であるSEAアルゴリズム(従来例2)においては、多項式剰余環上の乗算の計算量が大きいうという欠点がある。

【0021】本発明は、以上の従来技術における問題点を鑑みて行われたもので、多項式環上の乗算の計算時間を短縮することにより、楕円曲線の位数計算の計算時間を短縮し、これにより安全な公開鍵暗号及び署名方式を提供することを目的とする。

【0022】

【課題を解決するための手段】請求項1における発明は、予め与えられた有限体  $GF(p)$  の拡大体  $GF(q)$  ( $q=p^n$ ) 上の予め与えられた多項式  $r(X)$  (次数  $d$ ) を法とする1変数多項式剰余環  $GF(q)[X]/(r(X))$  において、 $R$  に属する多項式  $X$ 、 $f(X)$  を入力とし、 $R$  に属する多項式  $X^q$ 、 $f(X)^{((q-1)/2)}$  を出力する多項式演算装置であって、前記多項式  $X$  に対して、 $X^p$ 、 $X^{(2p)}$ 、 $X^{(3p)}$ 、 $\dots$ 、 $X^{((d-1)p)}$  を計算する第1乗算計算手段と、 $f(X)^{((q-1)/2)}$  を計算する第2乗算計算手段を備え、前記第2乗算計算手段は、前記第1乗算計算手段から出力される結果を用いることを特徴とする(ただし、 $p^n \nmid \Delta p(n \times \text{乗を示す})$ )。

【0023】請求項2における発明は、請求項1の第2乗算計算手段は、 $f(X)^{((p-1)/2)}$  を計算する中間計算を行ってから、前記第1乗算計算手段から出力される結果を用いて、 $f(X)^{((p^2-1)/2)} = f(X)^{(p)} \times f(X)^{((p-1)/2)}$ 、 $f(X)^{((p^3-1)/2)} = f(X)^{(p^2)} \times f(X)^{((p-1)/2)}$ 、 $\dots$ 、 $f(X)^{((p^n-1)/2)} = f(X)^{(p^{n-1})} \times f(X)^{((p-1)/2)}$  により計算することとを特徴とする。

【0024】請求項3における発明は、予め与えられた有限体  $GF(p)$  の拡大体  $GF(q)$  ( $q=p^n$ ) 上の楕円曲線を入力とし、前記楕円曲線の位数を出力する楕円曲線位数計算装置であって、予め与えられた初期値を設定する初期値設定部と、位数の情報を求める楕円曲線位数情報計算部と、前記楕円曲線位数情報計算部の終了判定を行う計算

終了判定部と、前記楕円曲線位数情報計算部から出力される情報を用いて楕円曲線の位数を決定する楕円曲線位数決定部を備え、前記楕円曲線位数情報計算部は、請求項1に記載の多項式演算装置を有することを特徴とする。

【0025】請求項4における発明は、予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上の楕円曲線を入力とし、前記楕円曲線の位数を出力する楕円曲線位数計算装置であって、予め与えられた初期値を設定する初期値設定部と、位数の情報を求める楕円曲線位数情報計算部と、前記楕円曲線位数情報計算部の終了判定を行う計算終了判定部と、前記楕円曲線位数情報計算部から出力される情報を用いて楕円曲線の位数を決定する楕円曲線位数決定部を備え、前記楕円曲線位数情報計算部は、請求項2に記載の多項式演算装置を有することを特徴とする。

【0026】請求項5における発明は、予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を出力する楕円曲線生成装置であって、予め与えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部を備え、前記楕円曲線位数計算部は、請求項3に記載の楕円曲線位数計算装置を有することを特徴とする。

【0027】請求項6における発明は、予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を出力する楕円曲線生成装置であって、予め与えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部を備え、前記楕円曲線位数計算部は、請求項4に記載の楕円曲線位数計算装置を有することを特徴とする。

【0028】請求項7における発明は、予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を用いる楕円曲線略号システムであって、予め与えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部を備え、前記楕円曲線位数計算部は、請求項3に記載の楕円曲線位数計算装置を有する楕円曲線生成装置により、生成されることを特徴とする。

【0029】請求項8における発明は、予め与えられた有限体GF(p)の拡大体GF(q) ( $q=p^n$ ) 上で定義され、予め与えられた条件を満たす楕円曲線を用いる楕円曲線略号

システムであって、予め与えられた楕円曲線設定値に基づいて、楕円曲線を設定する楕円曲線設定部と、前記有限体上の楕円曲線の位数を計算する楕円曲線位数計算部と、前記楕円曲線設定部で設定した楕円曲線を、前記与えられた条件で判定する楕円曲線条件判定部を備え、前記楕円曲線位数計算部は、請求項4に記載の楕円曲線位数計算装置を有する楕円曲線生成装置により、生成されることを特徴とする。

【0030】

【発明の実施の形態】図1は、本実施形態における多項式演算装置の構成を示すブロック図である。

【0031】この多項式演算装置は、従来例2のSEAアルゴリズムの多項式剰余環上の幕乗演算を実現するものであり、GF(q) ( $q=p^n$ ; p:素数)を有限体、Xを変数とし、G F(q) (係数である予め与えられたr(X) (次数d)を法とする1変数多項式剰余環=GF(q) (X)/r(X))において、Rに属する多項式Xとf(X)を入力とし、 $X^q$ とf(X)<sup>(q-1)/2</sup>を出力するものである。

【0032】多項式演算装置40は、第1幕乗計算部401と、第2幕乗計算部402と、第3幕乗計算部403と、第4幕乗計算部404を備える。

【0033】第1幕乗計算部401は、Rに属するXを入力とし、 $X^p$ 、 $X^{(2p)}$ 、 $X^{(3p)}$ 、...、 $X^{((d-1)p)}$ を計算し、出力する。

【0034】第2幕乗計算部402は、Rに属するXと第1幕乗計算部401から出力された $X^p$ 、 $X^{(2p)}$ 、...、 $X^{((d-1)p)}$ を入力とし、 $X^q$ を出力する。

【0035】第3幕乗計算部404は、Rに属するf(X)と第1幕乗計算部401から出力された $X^p$ 、 $X^{(2p)}$ 、...、 $X^{((d-1)p)}$ を入力とし、f(X)<sup>(q-1)/2</sup>を計算する。

【0036】第2幕乗計算部402の構成)図2は、第2幕乗計算部402の構成を示すブロック図である。

【0037】第2幕乗計算部402は、Rに属するXと第1幕乗計算部401から出力された $X^p$ 、 $X^{(2p)}$ 、...、 $X^{((d-1)p)}$ を入力とし、 $X^q$ を出力する多項式演算装置である。

【0038】第2幕乗計算部402は、初期値設定部4021と、多項式変換部4022と、終了判定部4023を備える。

【0039】初期値設定部4021は、 $c=1$  (cはカウンタ)、 $g(X)=X^q$ に設定する。

【0040】多項式変換部4022は、 $g(X)$ と第1幕乗計算部401から出力された $X^p$ 、 $X^{(2p)}$ 、...、 $X^{((d-1)p)}$ を入力とし、 $(g(X))^p$ を計算し、 $g(X)$ に改めおく。

【0041】多項式変換部4022では以下の計算を行う。

【0042】 $(g(X))^p = g_0 + g_1 X^p + g_2 X^{2p} + \dots + g_{(d-1)} X^{(d-1)p}$

ここで、 $g(X) = g_0 + g_1 X + g_2 X^2 + \dots + g_{(d-1)} X^{(d-1)}$  ( $g_0, g_1, \dots, g_{(d-1)}$ はGF(q)の元)であるとして仮定している。

【0043】終了判定部4023は、 $c=n$ であるか否かを判定する。

【0044】以下に、第2幕乗計算部402の動作を示す。

【 0 0 4 5 】初期値計算部4021は、カウンタ $c=1$ 、 $g(X)=X^p$ に設定し、多項式変換部4022に $g(X)$ と第1幕乗計算部401から出力された $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$ を入力する。多項式変換部4022は、 $(g(X))^p$ を計算し、 $g(X)$ に改めておく。終了判定部で4023は、 $c=n$ であるか否かを判定し、 $c=n$ であるときは、 $g(X)$ を出力し、終了。それ以外は、 $c$ に $c+1$ を改めておき、多項式変換部4022に戻る。

【 0 0 4 6 】(第3幕乗計算部403の構成)図3は、第3幕乗計算部403の構成を示すブロック図である。

【 0 0 4 7 】第3幕乗計算部403は、 $R$ に属する $f(X)$ と第1幕乗計算部401から出力された $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$ を入力とし、 $f(X)^{(q-1)/2}$ を計算する多項式演算装置である。

【 0 0 4 8 】第3幕乗計算部403は、中間計算部4031と、初期値設定部4032と、多項式変換部4033と、多項式乗算部4034と、終了判定部4035を備える。

【 0 0 4 9 】中間計算部4031は、 $f(X)^{(p-1)/2}$ を計算する。

【 0 0 5 0 】初期値設定部4032は、 $c=1$ 、 $g(X)=f(X)^{(p-1)/2}$ に設定する。

【 0 0 5 1 】多項式変換部4033は、多項式変換部4022と同一である。

【 0 0 5 2 】多項式乗算部4034は、 $g(X)$ と $f(X)^{(p-1)/2}$ を乗算する。

【 0 0 5 3 】終了判定部4035は、 $c=n$ であるか否かを判定する。

【 0 0 5 4 】以下に、第3幕乗計算部403の動作を示す。

【 0 0 5 5 】中間計算部4031は、 $f(X)^{(p-1)/2}$ を計算し、出力する。初期値計算部4032は、カウンタ $c=1$ 、 $g(X)=f(X)^{(p-1)/2}$ に設定し、多項式変換部4033に $g(X)$ と第1幕乗計算部401から出力された $X^p, X^{(2p)}, \dots, X^{((d-1)p)}$ を入力する。多項式変換部4033は、 $(g(X))^p$ を計算し、 $g(X)$ に改めておく。多項式乗算部4034で、 $g(X)$ と $f(X)^{(p-1)/2}$ を乗算し、 $g(X)$ に改めておく。終了判定部4035は、 $c=n$ であるか否かを判定し、 $c=n$ であるときは、 $g(X)$ を出力し、終了。それ以外は、 $c$ に $c+1$ を改めておき、多項式変換部4033に戻る。

【 0 0 5 6 】以下に、本多項式演算装置40の動作を示す。

【 0 0 5 7 】本装置が起動されると、まず、第1幕乗計算部401は $X^p, X^{(2p)}, X^{(3p)}, \dots, X^{((d-1)p)}$ を計算し出力する。第2幕乗計算部402は、第1幕乗計算部401から出力された $X^p, X^{(2p)}, X^{(3p)}, \dots, X^{((d-1)p)}$ と $X$ を入力とし、 $X^q$ を計算し出力する。次に第3幕乗計算部403は、第1幕乗計算部401から出力された $X^p, X^{(2p)}, X^{(3p)}, \dots, X^{((d-1)p)}$ と $X$ を入力とし、 $f(X)^{(q-1)/2}$ を計算し、 $X^q$ と $f(X)^{(q-1)/2}$ を出力する。

【 0 0 5 8 】この例の計算量について説明する。本実施形態は従来例2のSEAアルゴリズムで用いられる。以下で、従来の方法との比較を行う。

【 0 0 5 9 】多項式乗算の計算量を $P_{mul}$ とする。従来の方法では、 $f(X)^{(q-1)/2}$ を単に幕乗を行うことにより、求めていた。この場合、計算量は $3/2 \cdot q \cdot P_{mul}$ である( $q$ は $q$ のビット数)。それに対して、本実施形態では、中間計算部4031の計算量は、 $3/2 \cdot p \cdot P_{mul}$ ( $p$ は $p$ のビット数)であり、多項式変換部4033の計算量は $1 \times P_{mul}$ 、多項式乗算部4034の計算量は $1 \times P_{mul}$ であり、多項式変換部4043と多項式乗算部4044は、 $n-1$ 回繰り返すので、全体の計算量は、 $(3/2 \cdot p + 2 \times n - 2) \times P_{mul}$ である。 $q=160$ 、 $p=32$ 、 $n=5$ の場合、従来の方法では、 $f(X)^{(q-1)/2}$ を求める計算量は、 $240 \times P_{mul}$ であり、本実施形態1では、 $56 \times P_{mul}$ である。したがって、 $f(X)^{(p-1)/2}$ の計算が高速な多項式演算装置の効果は大きい。なお、本実施形態を用いた位数計算装置、楕円曲線生成装置並びに、楕円曲線暗号システムが実現可能となる。

【 0 0 6 0 】

【発明の効果】以上に説明したように本発明は、従来例における問題点を鑑みて行われたもので、SEAアルゴリズムにおいては、多項式環上の幕乗演算の計算時間を短縮できた。

【 0 0 6 1 】以上により、高速に安全な暗号方式や署名方式を可能にする楕円曲線生成装置を提供することができ、その実用価値は大きい。

【図面の簡単な説明】

【図1】本発明の実施形態における多項式演算装置のブロック図

【図2】本発明の実施形態における第2幕乗計算部402の構成を示すブロック図

【図3】本発明の実施形態における第3幕乗計算部403の構成を示すブロック図

【図4】従来例1の楕円曲線生成装置のブロック図

【図5】従来例2のSEAアルゴリズムによる楕円曲線位数計算装置のブロック図

【図6】従来例3の多項式演算装置のブロック図

【符号の説明】

10 従来例1の楕円曲線生成装置

101 乱数生成部

102 楕円曲線設定部

103 楕円曲線位数計算部

104 楕円曲線条件判定部

20 従来例2のSEAアルゴリズムによる楕円曲線位数計算装置

201 初期値設定部

202 楕円曲線位数情報計算部

203 計算終了判定部

204 楕円曲線位数決定部

30 従来例3の多項式演算装置

301 第1幕乗計算部

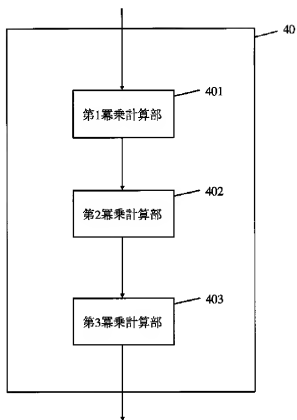
302 第2幕乗計算部

40 本発明の実施形態1の多項式演算装置

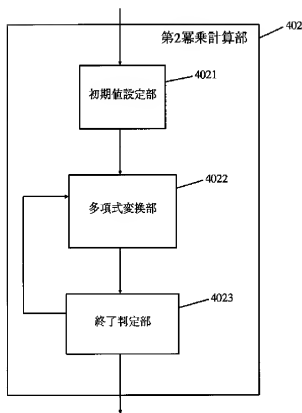
401 第1乗乗計算部  
 402 第2乗乗計算部  
 4021 初期値設定部  
 4022 多項式変換部  
 4023 終了判定部  
 403 第3乗乗計算部

4031 中間計算部  
 4032 初期値設定部  
 4033 多項式変換部  
 4034 多項式乗算部  
 4035 終了判定部

【図1】

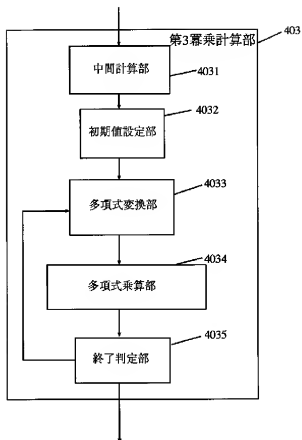


【図2】

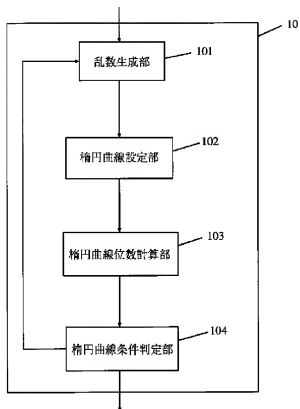




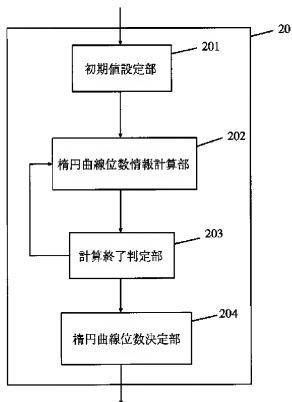
【図3】



【図4】



【図5】



【図6】

